FORTINET

Release Notes

FortiSwitchOS 7.2.3

FORTINET DOCUMENT LIBRARY
https://docs.fortinet.com

FORTINET VIDEO GUIDE
https://video.fortinet.com

FORTINET BLOG
https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT
https://support.fortinet.com

FORTINET TRAINING & CERTIFICATION PROGRAM
https://www.fortinet.com/training-certification

NSE INSTITUTE
https://training.fortinet.com

FORTIGUARD CENTER
https://www.fortiguard.com

END USER LICENSE AGREEMENT
https://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK
Email: techdoc@fortinet.com

March 1, 2023
FortiSwitchOS 7.2.3 Release Notes
11-723-847331-20230301

TABLE OF CONTENTS

Change log **4**
Introduction **5**
Supported models 5
What's new in FortiSwitchOS 7.2.3 6
Special notices **8**
Zero-touch management 8
By default, auto-network is enabled in FortiSwitchOS 7.2.0 and later 8
Downgrading FortiSwitchOS 7.0.0 and later to versions earlier than 6.2.6 or 6.4.4 is not supported 8
Downgrading FortiSwitchOS 7.0.0 and later requires converting the admin password first 8
Connecting multiple FSR-112D-POE switches 9
Upgrade information **10**
Product integration and support **11**
FortiSwitchOS 7.2.3 support 11
Resolved issues **12**
Common vulnerabilities and exposures 13
Known issues **14**

Change log

Date	Change Description
December 12, 2022	Initial release for FortiSwitchOS 7.2.3
December 14, 2022	Added bug 866231 as a resolved issue.
December 15, 2022	Added bugs 861167and 838908 as resolved issues.
December 16, 2022	• Updated the description of bug 793145. • Added bug 867108.
March 1, 2023	Revised the description of bug 857391.

Introduction

This document provides the following information for FortiSwitchOS 7.2.3 build 0434.

- Supported models on page 5
- Special notices on page 8
- Upgrade information on page 10
- Product integration and support on page 11
- Resolved issues on page 12
- Known issues on page 14

See the Fortinet Document Library for FortiSwitchOS documentation.

Supported models

FortiSwitchOS 7.2.3 supports the following models:

FortiSwitch 1xx	FS-108E, FS-108E-POE, FS-108E-FPOE, FS-108F, FS-108F-POE, FS-108F-FPOE, FS-124E, FS-124E-POE, FS-124E-FPOE, FS-124F, FS-124F-POE, FS-124F-FPOE, FS-148E, FS-148E-POE, FS-148F, FS-148F-POE, FS-148F-FPOE
FortiSwitch 2xx	FS-224D-FPOE, FS-224E, FS-224E-POE, FS-248D, FS-248E-POE, FS-248E-FPOE
FortiSwitch 4xx	FS-424E, FS-424E-POE, FS-424E-FPOE, FS-424E-Fiber, FS-M426E-FPOE, FS-448E, FS-448E-POE, FS-448E-FPOE
FortiSwitch 5xx	FS-524D, FS-524D-FPOE, FS-548D, FS-548D-FPOE
FortiSwitch 1xxx	FS-1024D, FS-1024E, FS-1048E, FS-T1024E
FortiSwitch 3xxx	FS-3032E
FortiSwitch Rugged	FSR-112D-POE, FSR-124D

What's new in FortiSwitchOS 7.2.3

Release 7.2.3 provides the following new features:

- You can now use the GUI to create a policy to control routing using the *Router* > *Config* > *Policy* > *Next Hop Groups*, *Router* > *Config* > *Policy* > *PBR Maps*, and *Router* > *Config* > *Policy* > *Interfaces* pages.
- IPv6 address are now supported in access control lists (ACLs) for ingress policies.
- To support the EtherLike-MIB, the following improvements have been made to the dot3StatsTable (OID: 1.3.6.1.2.1.10.7.2.1.19):
  - System interfaces are now supported in addition to switch ports.
  - The table type was changed from the simple table type to the complex table type so that the table size more accurately reflects the number of available interfaces.
  - The following additional nodes are now supported:
    - dot3StatsFCSErrors
    - dot3StatsDeferredTransmissions
    - dot3StatsInternalMacTransmitErrors
    - dot3StatsCarrierSenseErrors
    - dot3StatsFrameTooLongs
    - dot3StatsInternalMacReceiveErrors
  - There are additional diagnose-debug messages.
- PSK-mode MACsec and dynamic-CAK mode are now supported on the 10G and 100G ports on FS-1024E and the 100G ports on FS-T1024E. The FS-1024E and FS-T1024E models support the GCM-AES-128, GCM-AES-256, GCM-AES-XPN-128, and GCM-AES-XPN-256 cipher suites.
- The `set eap-egress-tagged {enable | disable}` command is now supported on the FS-1xxE and FS-1xxF models. When you are using the MAC move feature with EAP authentication, you can disable `eap-egress-tagged` to force the switch to always use the untagged EAP response.
- The following changes and enhancements have been made to the `set allow-mac-move` command:
  - The `set allow-mac-move` command has been changed to `set allow-mac-move-to` for FSR-124D, 200 Series, FS-4xxE, 500 Series, FS-1024D, FS-1024E, FS-T1024E, FS-1048E, and FS-3032E.
  - You can now use the `set allow-mac-move-from` command for the FS-108E, FS-108E-POE, FS-108E-FPOE, FS-108F, FS-108F-POE, FS-108F-FPOE, FS-124E, FS-124E-POE, FS-124E-FPOE, FS-148E, and FS-148E-POE models.
  - You can now enable the `set allow-mac-move` command on a global level for the FS-124F, FS-124F-POE, FS-124F-FPOE, FS-148F, FS-148F-POE, and FS-148F-FPOE models.
- The new *User*, *Security*, and *Fortinet* columns in the 802.1X *Session* page provide the user name, the security group name, and the RADIUS group name.
- You can now change how the ALARM LED functions for the FSR-112D-POE model, system part number P17080-04 or later. You can check the system part number with the `get system status` command. Use the following command to have the ALARM LED turn red when only one power supply unit (PSU) is connected:

  ```
  config system global
     set single-psu-fault enable
  end
  ```

  By default, the `set single-psu-fault` command is disabled.
- MAB-only authentication is now supported. In this mode, the FortiSwitch unit performs MAB authentication without performing EAP authentication. EAP packets are not sent. To enable MAB-only authentication:

  ```
  config switch interface
  ```

```
    edit <interface_name>
      config port-security
        set port-security-mode {802.1X | 802.1X-mac-based}
        set mac-auth-bypass enable
        set auth-order MAB
      end
    next
end
```

Refer to the FortiSwitch feature matrix for details about the features supported by each FortiSwitch model.

Special notices

Zero-touch management

When a new FortiSwitch unit is started, by default, it will connect to the available manager, which can be a FortiGate device, FortiLAN Cloud, or FortiSwitch Manager. All ports are enabled for auto discovery. The “internal” interface is the DHCP client in all FortiSwitch models. If you do not want your FortiSwitch unit to be managed, you must disable the features that you do not want active.

By default, auto-network is enabled in FortiSwitchOS 7.2.0 and later

After an `execute factoryreset` command is executed on a FortiSwitch unit in standalone mode, the auto-network configuration is enabled by default. If you are not using auto-network, you must manually disable it:

```
config switch auto-network
   set status disable
end
```

Downgrading FortiSwitchOS 7.0.0 and later to versions earlier than 6.2.6 or 6.4.4 is not supported

Downgrading FortiSwitchOS 7.0.0 and later to FortiSwitchOS 6.2.6 and later 6.2 versions is supported. Downgrading FortiSwitchOS 7.0.0 and later to FortiSwitchOS 6.4.4 and later 6.4 versions is supported. Downgrading FortiSwitchOS 7.0.0 to versions earlier than FortiSwitchOS 6.2.6 or 6.4.4 is not supported.

Downgrading FortiSwitchOS 7.0.0 and later requires converting the admin password first

Because FortiSwitchOS 7.0.0 changed from SHA1 to SHA256 encryption for admin passwords, you need to convert the format of the admin password before downgrading from FortiSwitchOS 7.0.0 and later to an earlier FortiSwitchOS version.

If you do not convert the admin password before downgrading from FortiSwitchOS 7.0.0 and later, the admin password will not work after the switch reboots with the earlier FortiSwitchOS version.

The encrypted admin password in FortiSwitchOS 7.0.0 and higher starts with “SH2”, and the encrypted admin password for earlier FortiSwitchOS versions starts with “AK1”.

To convert the format of the admin password in FortiSwitchOS 7.0.0 and later before downgrading to an earlier FortiSwitchOS version:

1. Enter the following CLI command to convert the admin password from SHA256 to SHA1 encryption:

   ```
   execute system admin account-convert <admin_name>
   ```

2. Downgrade your firmware.

Connecting multiple FSR-112D-POE switches

The FSR-112D-POE switch does not support interconnectivity to other FSR-112D-POE switches using the PoE ports. Fortinet recommends using the SFP ports to interconnect switches.

Upgrade information

FortiSwitchOS 7.2.3 supports upgrading from FortiSwitchOS 3.5.0 and later.

For the FS-424E, FS-424E-POE, FS-424E-FPOE, FS-424E-Fiber, and FS-M426-FPOE models, there is a two-step upgrade process if you are upgrading from FortiSwitchOS 6.0.x or 6.2.x to 7.2.x:

1. Upgrade from FortiSwitchOS 6.0.x or 6.2.x to FortiSwitchOS 6.4.12 or later.
2. Upgrade from FortiSwitchOS 6.4.12 or later to 7.2.x.

If you do not follow the two-step upgrade process, the FortiSwitch unit will not start after the upgrade, and you will need to use the serial console to conclude the upgrade (BIOS and OS).

For FortiSwitch units managed by FortiGate units, refer to the *FortiLink Release Notes* for upgrade information.

Product integration and support

FortiSwitchOS 7.2.3 support

The following table lists FortiSwitchOS 7.2.3 product integration and support information.

Web browser	• Mozilla Firefox version 52 • Google Chrome version 56 Other web browsers may function correctly, but are not supported by Fortinet.
FortiOS (FortiLink Support)	Refer to the FortiLink Compatibility table to find which FortiSwitchOS versions support which FortiOS versions.

Resolved issues

The following issues have been fixed in FortiSwitchOS 7.2.3. For inquiries about a particular bug, please contact Customer Service & Support.

Bug ID	Description
806907	Packet loss occurs when using the SP-CABLE-FS-SFP+5 direct-attach cable with FS-124F switches.
818628	When Virtual Router Redundancy Protocol (VRRP) is being used in a layer-3 MCLAG topology, static routes disappear after the FortiSwitch unit is restarted.
833450	Layer-2 multicast traffic is flooding to ports within the same VLAN, even though IGMP snooping is enabled.
833503	The FortiGate device does not detect a standalone FS-224E-POE that is running FortiSwitchOS 7.0.5.
834930	The `diagnose switch mclag peer-consistency-check` command displays split ports incorrectly.
837168	The following switches make a high fan noise: • FS-224D-FPOE • FS-224E-POE • FS-248D
838908, 861167	The event log erroneously reports “FAN failure detected” on multiple FS-248E-POE switches.
844973	After the firmware is successfully uploaded, the FS-M426E switch fails to upgrade.
845190	FortiSwitchOS will not allow `https` to be removed from the `set allowaccess` configuration.
846994	Configuring the `set group-name` under `config match` for `config user tacacs+` does not work.
849465	Using FN-TRAN-GC with the FS-108E or FS-108F switch causes link flapping or wrongly shows that the link is up when the cable is not connected.
850859	FortiSwitchOS sends the wrong OID for the SNMPv3 trap for link-down events.
857391	After upgrading FortiSwitchOS, multiple FS-448E switches report that the fan has failed, although the fan status is OK.
861492	The mgmt interface MAC address is set to 00:01:02:03:04:05 after a reboot or factory reset.
863009	When running FortiSwitchOS 7.2.2, the RPS LED does not light with the appropriate color when a redundant power supply is inserted.
866231	The `set status down` command (under `config switch physical-port`) does not work on the SFP+ ports on the FS-426E-FPOE for certain versions of FortiSwitchOS. If you need to shut down any of the SFP+ ports on the FS-426E-FPOE, do not use FortiSwitchOS 7.0.5, 7.2.0, 7.2.1, or 7.2.2.

Common vulnerabilities and exposures

Visit https://fortiguard.com/psirt for more information.

Bug ID	CVE references
855445	FortiSwitchOS 7.2.3 is no longer vulnerable to the following CVE Reference: • CVE-2022-3602

Known issues

The following known issues have been identified with FortiSwitchOS 7.2.3. For inquiries about a particular bug or to report a bug, please contact Fortinet Customer Service & Support.

Bug ID	Description
382518, 417024, 417073, 417099, 438441	DHCP snooping and dynamic ARP inspection (DAI) do not work with private VLANs (PVLANs).
414972	IGMP snooping might not work correctly when used with 802.1x Dynamic VLAN functionality.
480605	When DHCP snooping is enabled on the FSR-112D-POE, the switched virtual interface (SVI) cannot get the IP address from the DHCP server. **Workarounds:** —Use a static IP address in the SVI when DHCP snooping is enabled on that VLAN. —Temporarily disable dhcp-snooping on vlan, issue the `execute interface dhcpclient-renew <interface>` command to renew the IP address. After the SVI gets the IP address from the DHCP server, you can enable DHCP snooping.
510943	The time-domain reflectometer (TDR) function (cable diagnostics feature) reports unexpected values. **Workaround:** When using the cable diagnostics feature on a port (with the `diagnose switch physical-ports cable-diag <physical port name>` CLI command), ensure that the physical link on its neighbor port is down. You can disable the neighbor ports or physically remove the cables.
542031	For the 5xx switches, the `diagnose switch physical-ports led-flash` command flashes only the SFP port LEDs, instead of all the port LEDs.
548783	Some models support setting the mirror destination to “internal.” This is intended only for debugging purposes and might prevent critical protocols from operating on ports being used as mirror sources.
572052	Backup files from FortiSwitchOS 3.x that have 16-character-long passwords fail when restored on FortiSwitchOS 6.x. In FortiSwitchOS 6.x, file backups fail with passwords longer than 15 characters. **Workaround:** Use passwords with a maximum of 15 characters for FortiSwitchOS 3.x and 6.x.
585550	When packet sampling is enabled on an interface, packets that should be dropped by uRPF will be forwarded.

Bug ID	Description
606044/610149	The results are inaccurate when running cable diagnostics on the FS-108E, FS-124E, FS-108E-POE, FS-108E-FPOE, FS-124E-POE, FS-124E-FPOE, FS-148E, and FS-148E-POE models.
609375	The FortiSwitchOS supports four priority levels (critical, high, medium, and low); however, The SNMP Power Ethernet MIB only supports three levels. To support the MIB, a power priority of medium is returned as low for the PoE MIB.
659487	The FS-108E, FS-108E-POE, FS-108E-FPOE, FS-108F, FS-108F-POE, FS-108F-FPOE, FS-124E, FS-124E-POE, FS-124E-FPOE, FS-124F, FS-124F-POE, and FS-124F-FPOE, FS-148E, and FS-148E-POE models support ACL packet counters but not byte counters. The `get switch acl counters` commands always show the number of bytes as 0.
667079	For the FSR-112D-POE model: • If you have enabled IGMP snooping or MLD snooping, the FortiSwitch unit does not support IPv6 features and cannot pass IPv6 protocol packets transparently. • If you want to use IGMP snooping or MLD snooping with IPv6 features, you need to enable `set flood-unknown-multicast` under the `config switch global` command.
673433	Some 7-meter direct-attach cables (DACs) cause traffic loss for the FS- 448E model.
748210	The MAC authentication bypass (MAB) sometimes does not work on the FS-424E when a third-party hub is disconnected and then reconnected.
784585	When a dynamic LACP trunk has formed between switches in an MRP ring, the MRP ring cannot be closed. Deleting the dynamic LACP trunk does not fix this issue. MRP supports only physical ports and static trunks; MRP does not support dynamic LACP trunks. **Workaround:** Disable MRP and then re-enable MRP.
793145	VXLAN does not work with the following: • log-mac-event • DHCP snooping • LLDP-assigned VLANs • NAC • Block intra-VLAN traffic
829807	eBGP does not advertise routes to its peer by default unless the `set ebgp-requires-policy disable` command is explicitly configured or inbound/outbound policies are configured.
833450	Do not use multicast IP addresses in the ranges of 224-239.0.0.x and 224-239.128.0.x on the FS-2xxD, FS-2xxE, FS-4xxD, and FS-4xxE models.
867108	Depending on your browser type/version, web UI access might fail when using TLS 1.3 and client certificate authentication. **Workaround:** Use TLS 1.2.

www.fortinet.com